CERTIFICATION OF FACSIMILE TRANSMISSION

I hereby certify that this paper is being facsimile transmitted to the USPTO at (571-273-8300) on the date shown below.

Sept. 26 2011
Date

Francis C. Hand

Art Unit 2492

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Examiner:	Zachary A. Davis
Applicants:	Valene Skerpac
Serial No:	10/062,799
Filed:	January 31, 2002
Title :	N-Dimensional Biometric Security System

Customer No.:27172

APPEAL BRIEF

Sir:

This is an Appeal from the Final Rejection dated April 1, 2011 of claims 1, 2, 4 to 8, 10, 11, 13, 14 and 16 to 18.

The Appeal Brief filing fee of $270.00 (small entity) is to be charged to Deposit Account 03-0678 along with any additional fees.

REAL PARTY IN INTEREST

The real party in interest is the Applicant, Valene Skerpac

RELATED APPEALS AND INTERFERENCES

There are no related Appeals or Interferences.

STATUS OF CLAIMS

Claims1, 2, 4 to 8, 10, 11, 13, 14 and 16 to 18 have been rejected and are under appeal.

STATUS OF AMENDMENTS

All amendments to the claims have been entered.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1

Claim 1 is directed to a N-dimensional biometric security system. (page 6 ,ll. 5-6; Fig. 1 filed April 23, 2007)

The N-dimensional biometric security system comprises a station for receiving information representative of a user from the user and generating a signal responsive thereto; (page 6, ll. 11-12; 20-21) a first data base having a plurality of words and language rules for randomly generating one-time challenge phrases (page 6, ll. 12-13) from the words wherein each word of a randomly generated phrase is randomly generated; a second data base having biometric models of the user therein; (page 6, ll. 14-15) and a controller to receive and validate said signal as representative of the user, (page 6, ll. 15-16).

The controller, in response to validation of said signal, communicates with the first data base for randomly generating a one-time challenge phrase from the plurality of words and language rules in the first data base and delivering the one-time challenge phrase to the station for the user to speak the one-time challenge phrase exactly (page 6, ll. 16- 18; page 6, last line-page 7, line 1; page 12, ll. 20-22; page 13, ll. 6-8, ll. 12-16; page 15, ll. 13-14).

The controller also communicates with the station to receive a spoken response from the user to the delivered one-time challenge phrase and to generate a second signal representative of the spoken response;(page 7, ll. 2-3) to process the entire second signal for speaker recognition and to issue a first validation signal in response to a match between the second signal and the stored biometric model; to process the entire second signal for speech recognition and to issue a second validation signal in response to the second signal exactly matching the one-time challenge phrase; and to validate the spoken response to the one-time challenge phrase as representative of the user in response to receiving the first validation signal and the second validation signal. (page 9, l. 17 to page 10, l. 4; page 11, ll. 1-2; page 11, ll. 17-20)

Independent Claim 2

Claim 2 is directed to a method of identifying and validating a user comprising the steps of

initially inputting information representative of the user at a station, generating a first signal responsive to the information; receiving and validating the first signal as representative of the user; (page 6, ll. 11-12; 20-21)

thereafter, in response to validation of said first signal, generating and delivering a randomly generated one-time challenge phrase wherein each word of said phrase is randomly generated at said station for the user to speak exactly; (page 6, ll. 16- 18; page 6, last line-page 7, line 1; page 12, ll. 20-22; page 15, ll. 13-14; page 17, insert of July 31, 2007; Fig.1 of April 23, 2007)

generating a second signal representative of a spoken response to the challenge phrase; (page 17, insert of July 31, 2007; Fig.1 of April 23, 2007) thereafter receiving and simultaneously processing the entire second signal for each of speaker verification and speech recognition and issuing a first validation signal in response to speaker verification and a second validation signal in response to speech recognition; (page 17, insert of July 31, 2007; Fig.1 of April 23, 2007) and

validating the second signal as representative of the user in response to issuance of the first validation signal and the second validation signal. (page 17, insert of July 31, 2007; Fig.1 of April 23, 2007).

Independent Claim 4

Claim 4 is directed to a N-dimensional biometric security system. (page 6 ,ll. 5-6; Fig. 1 filed April 23, 2007)

The N-dimensional biometric security system comprises a station for receiving input information representative of a user from the user and generating a first signal responsive thereto; (page 6, ll. 11-12; 20-21) a first data base for storing a plurality of words and language rules for randomly generating one-time challenge phrases wherein each word of the phrase is randomly generated ; (page 6, ll. 12-13) a second data base for storing a biometric model of the user; (page 6, ll. 14-15) and a controller for receiving and validating the first signal as representative of the user, (page 6, ll. 15-16).

The controller is operatively connected to the first data base to, in response to the first signal, generate and deliver a one-time randomly generated challenge phrase to the station for the user to speak exactly. (page 6, ll. 16- 18; page 6, last line-page 7, line 1; page 12, ll. 20-22; page 13, ll. 6-8, ll. 12-16; page 15, ll. 13-14).

The controller also communicates with the station to receive and compare a spoken response to the challenge phrase with the entire challenge phrase to verify the spoken response as exactly matching the entire challenge phrase and to compare the spoken response to the stored biometric model of the user and for validating the spoken response as representative of the user in response to a match between the spoken response and the stored biometric model of the user. (page 9, l. 17 to page 10, l. 4; page 11, ll. 1-2; page 11, ll. 17-20; page 17, insert of July 31, 2007; Fig.1 of April 23, 2007)

The controller issues an authentication signal in response to a verification of the spoken response as exactly matching the challenge phrase and a validation of the spoken response as representative of the user. (page 17, insert of July 31, 2007; Fig.1 of April 23, 2007)

Independent Claim 5

Claim 5 is directed to a method of identifying and validating a user comprising the steps of

storing a plurality of words and language rules for randomly generating challenge phrases in a first data base;(page 6, ll. 12-13)

storing a biometric model of each of a multiplicity of users in a second data base; (page 6, ll. 14-15)

receiving information representative of a user from the user at an input station and generating a first signal responsive thereto; (page 6, ll. 11-12; 20-21)

thereafter, in response to the first signal, randomly generating a one-time challenge phrase wherein each word of the phrase is randomly generated from the stored plurality of words and language rules and forwarding the one-time challenge phrase to the station for the user to speak exactly; (page 6, ll. 16- 18; page 6, last line-page 7, line 1; page 12, ll. 20-22; page 13, ll. 6-8, ll. 12-16; page 15, ll. 13-14).

receiving a spoken response to the one-time challenge phrase and comparing the spoken response to the entire one-time challenge phrase to verify the spoken response as exactly matching the one-time challenge phrase; (page 11, ll. 1-2; page 11, ll. 17-20; page 17, insert of July 31, 2007; Fig.1 of April 23, 2007)

comparing the spoken response to the stored biometric models to obtain a match between the spoken response and one of the stored biometric models and issuing a validation signal in response to a match between the spoken response and one of stored biometric models; and (page 11, ll. 1-2; page 11, ll. 17-20; page 17, insert of July 31, 2007; Fig.1 of April 23, 2007)

issuing an authentication signal in response to a verification of the spoken response as matching the one-time challenge phrase and issuance of the validation signal. (page 11, ll. 1-2; insert of July 31, 2007; Fig.1 of April 23, 2007).

Independent Claim 16

Claim 16 is directed to a speech N-dimensional biometric security system comprising

a first data base having a plurality of words and language rules for generating randomly determined one-time challenge phrases; (page 6, ll. 12-13)

a second data base having a biometric model of an authorized user; (page 6, ll. 14-15)

a station for receiving information indicative of a user and generating a first signal responsive thereto; (page 6, ll. 11-12; 20-21)and a controller connected to the first data base to, in response to the first signal, randomly generate a one-time challenge phrase wherein each word of the phrase is randomly generated from the plurality of words and language rules in the first data base and to deliver the one-time challenge phrase to the station for the user to speak the one-time challenge phrase exactly, and (page 6, ll. 16- 18; page 6, last line-page 7, line 1; page 12, ll. 20-22; page 13, ll. 6-8, ll. 12-16; page 15, ll. 13-14).

The controller also communicates with the station to receive a spoken response from the user of the delivered one-time challenge phrase to process the entire spoken response for biometric speaker recognition and to produce a first validation signal as representative of an authorized user in response to a match between the spoken response and the stored biometric model for an authorized user, and to simultaneously process the entire spoken response for speech recognition and to produce a second validation signal in response to the spoken response exactly matching the one-time challenge phrase. (page 9, l. 17 to page 10, l. 4; page 11, ll. 1-2; page 11, ll. 17-20; page 17, insert of July 31, 2007; Fig.1 of April 23, 2007)

The controller also issues a positive authentication signal as representative of an authorized user in response to the first validation signal and the second validation signal being simultaneously produced. (page 11, ll. 1-2; insert of July 31, 2007; Fig.1 of April 23, 2007).

Independent Claim 17

Claim 17 is directed to a speech N-dimensional biometric security system comprising a station for receiving information indicative of a present user and generating a first signal responsive thereto; (page 6, ll. 11-12; 20-21) a first data base having a plurality of words and language rules for randomly generating one-time challenge phrases; (page 6, ll. 12-13) a second data base having a plurality of biometric models, each said biometric model corresponding to a respective one of a plurality of authorized users; (page 6, ll. 14-15) and a controller to receive said first signal as indicative of the present user. (page 6, ll. 15-16).

The controller communicates with the first data base for randomly generating a one-time challenge phrase wherein each word of the phrase is randomly generated from the plurality of words and language rules in the first data base and delivering the one-time challenge phrase to the station for the present user to speak the one-time challenge phrase exactly, and (page 6, ll. 16- 18; page 6, last line-page 7, line 1; page 12, ll. 20-22; page 13, ll. 6-8, ll. 12-16; page 15, ll. 13-14).

The controller also communicates with the station to receive a spoken response from the present user of the delivered one-time challenge phrase to process the entire spoken response for biometric speaker recognition and to produce a first validation signal as representative of the present user being an authorized user in response to a match between the spoken response and the stored biometric model for the present user, to simultaneously process the spoken response for speech recognition and to produce a second validation signal as representative of the spoken response exactly matching the one-time challenge phrase. (page 9, l. 17 to page 10, l. 4; page 11, ll. 1-2; page 11, ll. 17-20; page 17, insert of July 31, 2007; Fig.1 of April 23, 2007)

The controller also issues a positive authentication signal as representative of the present user being an authorized user in response to the first validation signal and the second validation signal being simultaneously produced. (page 11, ll. 1-2; insert of

July 31, 2007; Fig.1 of April 23, 2007).

<u>Grounds of Rejection to be Reviewed on Appeal</u>

The ground of rejection to be reviewed is as follows:

1. Claims 1, 2, 4-8, 11, 14 and 16 -18 stand rejected under 35 USC 103(a0 as being unpatentable over Hattori (US6,094,632) in view of Higgins ("Speaker Verification Using Randomized Phrase Prompting")

<u>Argument</u>

Claim 1 requires, inter alia, a station for receiving information "representative of a user from the user and generating a signal responsive thereto" and a controller "to receive and validate said signal as representative of the user, said controller, in response to validation of said signal, ... delivering said one-time challenge phrase to said station for the user to speak said one-time challenge phrase ..."

<u>Hattori</u> does not disclose such structures. Instead, <u>Hattori</u> judges whether or not an unknown speaker is a genuine registered speaker (i.e. a customer), by instructing the unknown speaker to utter at least two kinds of things: a 'specified text' and a 'password'. (col. 8, l. 65 to Col. 9, l. 2) There is no disclosure of any station that receives information from a user to deliver a signal to a controller that, in response, delivers a one-time challenge phrase to the station for the user to speak.

See also <u>Hattori</u> at col. 14, l. 18, *et seq*

> "In the following, the operation of the speaker recognition device of FIG.5 will be described.
>
> The text generation section 201 generates a specified text to be uttered by an unknown speaker together with a password. The specified text generated by the text generation section 201 is presented to the unknown speaker by means of sound, image, etc. by the presentation

> section 202, and the unknown speaker is instructed to input an ID and utter the specified text and the password in series."

There is no disclosure in Hattori that the text generation section 201 receives a signal from the presentation section 202 in order to generate the specified text to be uttered by an unknown speaker.

The Examiner posits that Hattori discloses a station for receiving input information which is representative of a user from the user and for generating a signal responsive thereto citing co. 9, ll.5-11. However, this is not a disclosure that the text generation section 201 receives a signal from the presentation section 202 in order to generate the specified text *to be uttered* by an unknown speaker.

In view of the above, any modification of Hattori with the teachings of Higgins would not result in the claimed structure. Accordingly, a rejection of claim 1 as being unpatentable over Hattori in view of Higgins is not warranted pursuant to the provisions of 35 USC 103(a).

Claim 1 further requires "a first data base having a plurality of words and language rules for randomly generating one-time challenge phrases from said words wherein each word of a randomly generated phrase is randomly generated." The Examiner considers that Hattori a data base having a plurality of words and language rules for randomly generating one-time challenge phrases citing col. 9, ll. 19-47; col.8, l. 65 to col. 9, l.5 and col. 9., ll. 61-64. The Examiner is in error.

Hattori at col. 9, ll. 19-47 reads:

> As mentioned above, the speaker recognition device according to the present invention realizes avoidance of the imposture by voice recording with easy speaker registration and small storage capacity of the device, by combining two types of verification together, i.e. `text verification using speaker independent speech recognition` and `speaker verification by comparison with a reference

pattern of a password of a registered speaker`.

For the text verification using speaker independent speech recognition, a document: T. Watanabe et al. "Unknown utterance rejection using likelihood normalization based on syllable recognition", The Transactions of the Institute of Electronics, Information and Communication Engineers, vol. J75-D-II, No. 12, pages 2002-2009 (December 1992) (hereafter, referred to as `document No. 2`) is known. According to the document No. 2, inputted speech which ought not to be recognized as a word or a phrase (i.e., out of vocabulary words) can be rejected accurately by using two likelihoods. The first likelihood is a likelihood between an inputted speech input pattern of the inputted speech) and a reference pattern of a word (or a phrase) to be recognized. The second likelihood is a likelihood between the inputted speech (the input pattern of the inputted speech) and a reference pattern which can accept all possible phoneme sequence. The inputted speech is rejected as it ought not to be recognized if the difference between the first likelihood and the second likelihood is larger than a threshold value.

There is clearly no disclosure in the above citation from Hattori of a data base having a plurality of words and language rules for randomly generating one-time challenge phrases as required by claim 1.

Hattori at col. 9, ll. 19-47 reads:

> The speaker recognition device according to the present invention judges whether or not an unknown speaker is a genuine registered speaker (i.e. a customer), by instructing the unknown speaker to utter at least two kinds of things: a `specified text` and a `password`. The specified text is specified by the speaker recognition device or by the user of the device, and the password is decided by each speaker to be registered on speaker registration.

There is clearly no disclosure in the above citation from Hattori of a data base having a plurality of words and language rules for randomly generating one-time challenge phrases as required by claim 1. Note is made of the Examiner's reference to the "specified text" being provided to the user. However, there is no disclosure of the specific text being a randomly generated one-time challenge phrase. Instead, it appears that the "specified text" may be an oft- repeated text for multiple users.

Hattori at col. 9, ll. 19-47 reads:

> For example, the speaker recognition device may instruct the unknown speaker to utter a specified text and a password by displaying "Please say the date of today `December the twenty-fifth` and your password in series".

There is clearly no disclosure in the above citation from Hattori of a data base having a plurality of words and language rules for randomly generating one-time challenge phrases as required by claim 1.

For the above reasons, any modification of Hattori with the teachings of Higgins would not result in the claimed structure. Thus, a rejection of claim 1 as being unpatentable over Hattori in view of Higgins is not warranted pursuant to the provisions of 35 USC 103(a).

Claim 1 further requires the controller "to receive a spoken response from the user to said delivered one-time challenge phrase and **to generate a second signal** representative of the spoken response, **to process the entire said second signal for speaker recognition** and to issue a first validation signal in response to a match between said second signal and said stored biometric model, **to process the entire said second signal for speech recognition** and to issue a second validation signal in response to said second signal exactly matching said one-time challenge phrase ..." The Examiner considers that Hattori discloses a controller that communicates with the station to receive a spoken response and generate a second signal that represents the response citing col. 9, ll. 5-11. The Examiner is in error.

Hattori at col. 9, ll. 5-11 reads:

> The speaker recognition device inputs the specified text and the password uttered by the unknown speaker and an ID inputted by the unknown speaker, and judges whether or not the unknown speaker is an authentic registered

> speaker, using the text contents of the specified text uttered by the unknown speaker and acoustic features of the password uttered by the unknown speaker.

There is no disclosure in the above citation from Hattori of generating a second signal that represents the spoken response. Nor is there any disclosure in Hattori of processing the entire signal from the speaker recognition device for both speaker recognition and speech recognition as required by claim 1. Instead, processes the uttered text contents and the uttered password separately. See Hattori at col. 9, ll. 21-28

> As mentioned above, the speaker recognition device according to the present invention realizes avoidance of the imposture by voice recording with easy speaker registration and small storage capacity of the device, by combining two types of verification together, i.e. `text verification using speaker independent speech recognition' and `speaker verification by comparison with a reference pattern of a password of a registered speaker'.

For the above reason, any modification of Hattori with the teachings of Higgins would not result in the claimed structure. Thus, a rejection of claim 1 as being unpatentable over Hattori in view of Higgins is not warranted pursuant to the provisions of 35 USC 103(a).

The Examiner acknowledges that Hattori does not disclose that each word in the alleged one-time challenge phrase is randomly generated or processing the entire signal for both speech and speaker recognition. However, the Examiner posits that Higgins discloses a security system that includes a data base having a plurality of words and language rules for randomly generating one-time challenge phrases (citing page 90, section 2) and a controller that processes the entire signal received from the user for speaker recognition and speech recognition (citing pages 92-95, section 3.3).

Further, the Examiner considers that it would be obvious from Higgins to modify Hattori to include random phrase generation and processing of the entire signal for speaker recognition and speech recognition. The Examiner is in error.

First, Higgins describes the design requirements as including (1) an enrollment session taking no longer than 3 minutes and (4) prompts chosen at random from a large number of possibilities. (page 89, col. 1, first para.) Further, Higgins states "To address requirement (4), the system described here uses a prompting strategy in which phrases are composed at random using a small vocabulary of words. The spoken phrases are compared with word templates derived from enrollment sessions. (page 89, col. 1, second para.)

Higgins, at page 90, col. 1, discloses that a design strategy was chosen "to form phrases by concatenating words selected at random from a **small vocabulary.**" (emphasis added). The speech material chosen consisted of combination lock phrases (175,616 phrases) with a verification trial or session consisting of four such phrases. Enrollment requires speaking 24 such phrases, which typically takes about 3 minutes per enrollment session. Higgins discloses that prompted phrases are generated at random at the time when verification takes place.

Hence, Higgins teaches that an individual enrollee, at the time of enrollment, will speak only 24 phrases for the system to record for that individual. Higgins further teaches that it is only from these 24 phrases that an individual will be asked to utter a phrase for verification purposes when using the system. (page 90, col. 2, second para.)

Hence, since the Higgins system has only 24 phrases from which to select a phrase for verification, after 24 uses of the verification system by an individual, the phrases will be repeated. That is to say, the 24 phrases are not one-time challenge phrases as the Examiner posits.

Note is made that the Examiner disagrees and explains in the Advisory Action of April 1, 2011 "Higgins also discloses that for subsequent verification trials, any three numbers could be randomly selected to generate each verification phrase, and that is not limited to the 24 selected at enrollment." However, conducting a subsequent verification session has no relevance to the requirements of claim 1. Hence, the Examiner's explanation is not understood in the context of claim 1.

Second, claim 1 requires "a first data base having a plurality of words and language rules for randomly generating one-time challenge phrases from said words". Higgins, at page 90, col. 1, discloses that a design strategy was chosen "to form phrases by concatenating words selected at random from a **small vocabulary**" namely, "combination lock phrases" of three numbers between 21 and 97. There is no disclosure of employing language rules as required by claim 1.

In view of the above, the rejection of claim 1 as being unpatentable over Hattori in view of Higgins is not warranted.

It would not be obvious to modify the system of Hattori to include the random phrase generation as taught by Higgins

Hattori teaches that the speaker recognition device realizes avoidance of the imposture by combining two types of verification together, i.e. `text verification using speaker independent speech recognition` and `speaker verification by comparison with a reference pattern of a password of a registered speaker`. (Col. 9, lines 19-47).

Modifying Hattori to include the alleged random phrase generation of Higgins would require an individual to enroll in a verification session taking 3 minutes in order to provide the system with 24 phrases before the individual could attempt to access the system. This is contrary to the teachings of Hattori.

Also, modifying Hattori to include the alleged random phrase generation of Higgins would require an individual to speak a "specified text" that is selected from *only* 24 prerecorded phrases. However, the prerecorded phrase would not be a one-time challenge phrase for the reasons set forth above.

It would not be obvious to modify the system of Hattori to include the processing of the entire signal for speaker and speech recognition as taught by Higgins

Modifying Hattori to process the entire signal (i.e. the "specified text" and the password) for speaker and speech recognition as taught by Higgins would eliminate the teaching of Hattori of combining two types of verification together, i.e. `text verification using speaker independent speech recognition' and `speaker verification by comparison with a reference pattern of a password of a registered speaker'. If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959) [MPEP 2143.01 VI]. The Examiner's proposal would change the principle of operation of Hattori. For this reason alone, the proposed modification of Hattori would not be obvious to one of ordinary skill in the art.

Whether an invention would have been obvious under § 103 is a question of law based on underlying findings of fact. In re Kotzab, 217 F.3d 1365, 1369 (Fed. Cir. 2000). For a prima facie case of obviousness to exist, there must be "some objective teaching in the prior art or . . . knowledge generally available to one of ordinary skill in the art [that] would lead that individual to combine the relevant teachings of the references." In re Fine, 837 F.2d 1071, 1074 (Fed. Cir.1988). "The motivation, suggestion or teaching may come explicitly from statements in the prior art, the knowledge of one of ordinary skill in the art, or, in some cases the nature of the problem to be solved." Kotzab, 217 F.3d at 1370. The presence or absence of a motivation to combine references is a question of fact, In re Dembiczak, 175 F.3d 994, 1000 (Fed. Cir. 1999), which is evaluated under the substantial evidence standard. In re Gartside, 203 F.3d 1305, 1316 (Fed. Cir. 2000).

For the above reasons, a rejection of claim 1 as being unpatentable over Hattori in view of Higgins is not warranted pursuant to the provisions of 35 USC 103.

Claim 1 further requires "a controller ... in response to validation of said signal, communicating with said first data base for randomly generating a one-time challenge phrase from said plurality of words and language rules in said first data base". Higgins does not describe or teach such a structure. First, Higgins does not appear to disclose how any controller is activated. Second, Higgins does not communicate with a data base to generate a "prompted phrase" from a plurality of words and language rules but rather Higgins selects a "prompted phrase" from 24 prerecorded phrases. For this additional reason, a rejection of claim 1 as being unpatentable over Hattori in view of Higgins is not warranted pursuant to the provisions of 35 USC 103.

Claim 2

Claim 2 is directed to a method of identifying and validating a user and contains recitations similar to claim 1.

In particular, claim 2 requires "initially inputting information representative of the user at a station" and "generating a first signal responsive to the information". Neither Hattori nor Higgins appears to describe or teach such steps.

Claim 2 requires "thereafter, in response to validation of said first signal, generating and delivering a randomly generated one-time challenge phrase wherein each word of said phrase is randomly generated at said station ...". For reasons set forth above neither Hattori nor Higgins describes or teaches such a step.

Claim 2 requires "generating a second signal representative of a spoken response to said challenge phrase" and "thereafter receiving and simultaneously processing the entire second signal for each of speaker verification and speech recognition and issuing a first validation signal in response to speaker verification and a second validation signal in response to speech recognition". The Examiner acknowledges that Hattori does not describe or teach such a step. Further, for the reasons set forth above, it would not be obvious to modify Hattori to process the entire signal (i.e. the "specified text" and the password) for speaker and speech recognition from the teachings of Higgins.

Claim 4

Claim 4 contains recitations similar to claim 1 and is believed to be allowable for similar reasons.

Claim 5

Claim 5 contains recitations similar to claim 2 and is believed to be allowable for similar reasons.

Claims 6, 11 and 14

Claims 6, 11 and 14 depend from claim 5 and are believed to be allowable for similar reasons.

Claims 7 and 8

Claims 7 and 8 depend from claim 2 and are believed to be allowable for similar reasons.

Claim 16

Claim 16 contains recitations similar to claim 1 and is believed to be allowable for similar reasons.

Claim 17

Claim 17 contains recitations similar to claim 1 and is believed to be allowable for similar reasons.

Claim 18

Claim 18 depends from claim 4 and is believed to be allowable for similar reasons. Further, claim 18 requires "said first data base stores said plurality of words and language rules in a plurality of language sets, each said language set being specific to a subject area different from the subject areas of the other of said language sets." Hattori and Higgins are each void of any such teaching.

The passages of Hattori cited by the Examiner in support of the rejection are void of any teaching of words and language rules in a plurality of language sets or of any language sets of different subject areas. Note that Hattori discloses only that the "specific text" is "December the twenty-fifth" (see col. 9, lines 63-64).

For this additional reason, a rejection of claim 18 as being unpatentable over Hattori in view of Higgins is not warranted pursuant to the provisions of 35 USC 103.

Note is made of the objection to claims 1, 4 and 16-18 that the term "N-dimensional" is not defined in the claims. However, the term "N-dimensional" is a term coined by Applicant as defined in the Description at page 1, line 13 *et seq.* Accordingly, the objection is not understood.

CONCLUSION

Appellant has set forth definitive claims setting forth that which she believes her invention to be for the reasons expressed above.

Appellant's invention is not obvious to one of ordinary skill in the art from the references of record for the reasons expressed above.

Accordingly, a rejection of the claims on appeal is not warranted and the Final Rejection should be reversed..

Respectfully submitted,

Francis C. Hand
Francis C. Hand
Reg. No. 22,280

CARELLA, BYRNE BAIN, GILFILLAN,
CECCHI, STEWART & OLSTEIN
Five Becker Farm Road
Roseland, NJ 07068
Phone: 973-994-1700
Fax: 973-994-1744

USSN: 10/062,799
Filed : 01/31/2002

APPENDIX

1. A N-dimensional biometric security system comprising

a station for receiving information representative of a user from the user and generating a signal responsive thereto;

a first data base having a plurality of words and language rules for randomly generating one-time challenge phrases from said words wherein each word of a randomly generated phrase is randomly generated;

a second data base having biometric models of the user therein; and

a controller to receive and validate said signal as representative of the user, said controller, in response to validation of said signal, communicating with said first data base for randomly generating a one-time challenge phrase from said plurality of words and language rules in said first data base and delivering said one-time challenge phrase to said station for the user to speak said one-time challenge phrase exactly and said controller communicating with said station

to receive a spoken response from the user to said delivered one-time challenge phrase and to generate a second signal representative of the spoken response,

to process the entire said second signal for speaker recognition and to issue a first validation signal in response to a match between said second signal and said stored biometric model,

to process the entire said second signal for speech recognition and to issue a second validation signal in response to said second signal exactly matching said one-time challenge phrase, and

to validate the spoken response to said one-time challenge phrase as representative of the user in response to receiving said first validation signal and said second validation signal.

2. A method of identifying and validating a user comprising the steps of

initially inputting information representative of the user at a station;

generating a first signal responsive to the information;

receiving and validating said first signal as representative of the user;

thereafter, in response to validation of said first signal, generating and delivering a randomly generated one-time challenge phrase wherein each word of said phrase is randomly generated at said station for the user to speak exactly;

generating a second signal representative of a spoken response to said challenge phrase;

thereafter receiving and simultaneously processing the entire second signal for each of speaker verification and speech recognition and issuing a first validation signal in response to speaker verification and a second validation signal in response to speech recognition; and

validating the second signal as representative of the user in response to issuance of said first validation signal and said second validation signal.

4. A N-dimensional biometric security system comprising

a station for receiving input information representative of a user from the user and generating a first signal responsive thereto;

a first data base for storing a plurality of words and language rules for randomly generating one-time challenge phrases wherein each word of said phrase is randomly_generated ;

a second data base for storing a biometric model of the user; and

a controller for receiving and validating said first signal as representative of the user, said controller being operatively connected to said first data base to, in response to said first signal, generate and deliver a one-time randomly generated challenge phrase to said station for the user to speak exactly, said controller communicating with said station to receive and compare a spoken response to said challenge phrase with said entire challenge phrase to verify said spoken response as exactly matching said entire challenge phrase and to compare said spoken response to said stored biometric model of said user and for validating said spoken response as representative of said user in response to a match between said spoken response and said stored biometric model of said user, said controller issuing an authentication signal in response to a verification of said spoken response as exactly matching said challenge phrase and a validation of said spoken response as representative of said user.

5. A method of identifying and validating a user comprising the steps of

storing a plurality of words and language rules for randomly generating challenge phrases in a first data base;

storing a biometric model of each of a multiplicity of users in a second data base;

receiving information representative of a user from the user at an input station and generating a first signal responsive thereto;

thereafter, in response to said first signal, randomly generating a one-time challenge phrase wherein each word of said phrase is randomly generated from said stored plurality of words and language rules and forwarding said one-time challenge phrase to said station for the user to speak exactly;

receiving a spoken response to said one-time challenge phrase;

comparing said spoken response to said entire one-time challenge phrase to verify said spoken response as exactly matching said one-time challenge phrase;

comparing said spoken response to the stored biometric models to obtain a match between said spoken response and one of said stored biometric models,

issuing a validation signal in response to a match between said spoken response and one of said stored biometric models; and

issuing an authentication signal in response to a verification of said spoken response as matching said one-time challenge phrase and issuance of said validation signal.

6. A method as set forth in claim 5 wherein a user additionally selects a word phrase as a private and personal challenge phrase.

7. A method as set forth in claim 2 wherein a user additionally selects a word phrase as a private and personal challenge phrase.

8. A method as set forth in claim 2 further comprising the step of establishing a session time out limit in response to said first signal.

11. A method as set forth in claim 5 further comprising the step of establishing a session time out limit in response to said first signal.

14. A method as set forth in claim 5 further comprising the steps of encrypting and digitally signing said spoken response to said one-time challenge phrase after reception thereof and subsequently decrypting said spoken response prior to said step of comparing said spoken response to the stored biometric models.

16. A speech N-dimensional biometric security system comprising

a first data base having a plurality of words and language rules for generating randomly determined one-time challenge phrases;

a second data base having a biometric model of an authorized user;

a station for receiving information indicative of a user and generating a first signal responsive thereto; and

a controller connected to said first data base to, in response to said first signal, randomly generate a one-time challenge phrase wherein each word of said phrase is randomly generated from said plurality of words and language rules in said first data base and to deliver said one-time challenge phrase to said station for the user to speak said one-time challenge phrase exactly, and

said controller communicating with said station to receive a spoken response from the user of said delivered one-time challenge phrase

to process said entire spoken response for biometric speaker recognition and to produce a first validation signal as representative of an authorized user in response to a match between said spoken response and said stored biometric model for an authorized user, and to simultaneously process said entire spoken response for speech recognition and to produce a second validation signal in response to said spoken response exactly matching said one-time challenge phrase, and

said controller to issue a positive authentication signal as representative of an authorized user in response to said first validation signal and said second validation signal being simultaneously produced.

17. A speech N-dimensional biometric security system comprising

a station for receiving information indicative of a present user and generating a first signal responsive thereto;

a first data base having a plurality of words and language rules for randomly generating one-time challenge phrases;

a second data base having a plurality of biometric models, each said biometric model corresponding to a respective one of a plurality of authorized users; and

a controller to receive said first signal as indicative of the present user, said controller communicating with said first data base for randomly generating a one-time challenge phrase wherein each word of said phrase is randomly generated from said plurality of words and language rules in said first data base and delivering said one-time challenge phrase to said station for the present user to speak said one-time challenge phrase exactly, and

said controller communicating with said station to receive a spoken response from the present user of said delivered one-time challenge phrase to process said entire spoken response for biometric speaker recognition and to produce a first validation signal as representative of said present user being an authorized user in response to a match between said spoken response and said stored biometric model for said present user,

to simultaneously process said spoken response for speech recognition and to produce a second validation signal as representative of said spoken response exactly matching said one-time challenge phrase, and

said controller to issue a positive authentication signal as representative of said present user being an authorized user in response to said first validation signal and said second validation signal being simultaneously produced.

18. A N-dimensional biometric security system as set forth in claim 4 wherein said first data base stores said plurality of words and language rules in a plurality of language sets, each said language set being specific to a subject area different from the subject areas of the other of said language sets.

USSN: 10/062,799
Filed : 01/31/2002

EVIDENCE APPENDIX

-None-

USSN: 10/062,799
Filed : 01/31/2002

RELATED PROCEEDINGS APPENDIX

-None-